

# MIMO Secret Communications Against an Active Eavesdropper

Lingxiang Li, Athina P. Petropulu, *Fellow, IEEE*, Zhi Chen, *Member, IEEE*

**Abstract**—This paper considers a scenario in which an *Alice-Bob* pair wishes to communicate in secret in the presence of an active *Eve*, who is capable of jamming as well as eavesdropping in Full-Duplex (FD) mode. As countermeasure, *Bob* also operates in FD mode, using a subset of its antennas to act as receiver, and the remaining antennas to act as jammer and transmit noise. With a goal to maximize the achievable secrecy degrees of freedom (S.D.o.F.) of the system, we provide the optimal receive/transmit antennas allocation at *Bob*, based on which we determine in closed form the maximum achievable S.D.o.F.. We further investigate the adverse scenario in which *Eve* knows *Bob*'s transmission strategy and optimizes its transmit/receive antennas allocation in order to minimize the achievable S.D.o.F.. For that case we find the worst-case achievable S.D.o.F.. We also provide a method for constructing the precoding matrices of *Alice* and *Bob*, based on which the maximum S.D.o.F. can be achieved. Numerical results validate the theoretical findings and demonstrate the performance of the proposed method in realistic settings.

**Index Terms**—Physical-layer security, Cooperative communications, Multi-input Multi-output, Active Eavesdropper.

## I. INTRODUCTION

Communication security in the presence of malicious nodes has received a lot of attention. Most of the current literature addresses the case in which the malicious nodes are *passive* eavesdroppers, i.e., they just listen. In that case, the eavesdroppers reduce the secrecy rate by the rate they can sustain. Approaches to improve the secrecy rate in the presence of passive eavesdroppers include multi-antenna techniques [1]–[4] and artificial noise (jamming) based methods [5]–[13]; all these methods target at increasing the received signal-to-noise ratio (SNR) at the legitimate receiver, or decreasing the received SNR at the eavesdropper. Jamming can be implemented by the source [5], the external helper [6]–[11], or the legitimate receiver who may work in Full-Duplex (FD) mode [12], [13].

Recently, the case of *active* eavesdroppers has been receiving a lot of attention. By active eavesdropper we here refer to a powerful adversary that can jam as well as eavesdrop the legitimate receiver. One line of research in that area is gearing towards designing effective active attack schemes for the purpose of minimizing the achievable secrecy transmission rate [14]–[16]. Another line of research focuses on detecting

active attacks and offering countermeasures to guarantee reliable secret communications [17]–[23]. In particular, [17]–[19] consider a massive multi-input multi-output (MIMO) scenario, in which an active eavesdropper attacks the channel estimation process by transmitting artificial noise. [20], [21], [22], [23] consider a single-input single-output (SISO) scenario, a MIMO scenario, a relay scenario, and an OFDM scenario, respectively, wherein an active eavesdropper tries to reduce the total network throughput by choosing to be a jammer, or an eavesdropper, or combination of the above, so that it creates the most unfavorable conditions for secret communications. To combat such malicious behavior, the source in [20], [21] chooses between transmitting, remaining silent or acting as a jammer. The work of [22], [23] conducts relaying selection and power allocation among all the available sub-carriers, respectively.

In this paper, we consider a MIMO *Alice-Bob-Eve* wiretap channel, in which *Eve* is an active eavesdropper, who can transmit and receive in FD fashion by appropriately allocating its antennas for transmission or reception. Our goal is to provide countermeasures that will ensure maximum secrecy from the point of view of secrecy degrees of freedom (S.D.o.F.). Our main contributions are summarized as follows.

- 1) As countermeasure, we proposed an FD *Bob*, who transmits jamming signals while receiving. Under this scenario, we determine in closed form the maximum achievable S.D.o.F., as function of the number of antennas at each terminal (see eq. (6)). Moreover, we give the optimal transmit/receive antenna allocation of *Bob* (see (7)), which achieves the maximum S.D.o.F..
- 2) We obtain analytically the worst-case achievable S.D.o.F. (see eq. (9)), corresponding to the case in which *Eve* knows the strategy adopted by *Alice* and *Bob* and optimizes its transmit/receive antenna allocation for the purpose of minimizing the achievable S.D.o.F..
- 3) We provide a method for constructing the precoding matrix pair at *Alice* and *Bob*, which achieves the maximum S.D.o.F.. While the aforementioned achievable S.D.o.F. results do not depend on channel state information (CSI), the precoding matrices depend on the eavesdropping channels and also the null space of the self-interference channels at *Eve* and *Bob*.

The rest of this paper is organized as follows. In Section II, we describe the system model and formulate the S.D.o.F. maximization problem. In Section III, we determine in closed form the maximum achievable S.D.o.F., and provide an optimal transmission scheme which achieves the maximum S.D.o.F..

Lingxiang Li and Zhi Chen are with the National Key Laboratory of Science and Technology on Communications, UESTC, Chengdu 611731, China (e-mails: lingxiang.li@rutgers.edu; chen\_zhi@uestc.edu.cn). The work was performed when L. Li was a visiting student at Rutgers University.

Athina P. Petropulu is with the Department of Electrical and Computer Engineering, Rutgers–The State University of New Jersey, New Brunswick, NJ 08854 USA (e-mail: athinap@rci.rutgers.edu).

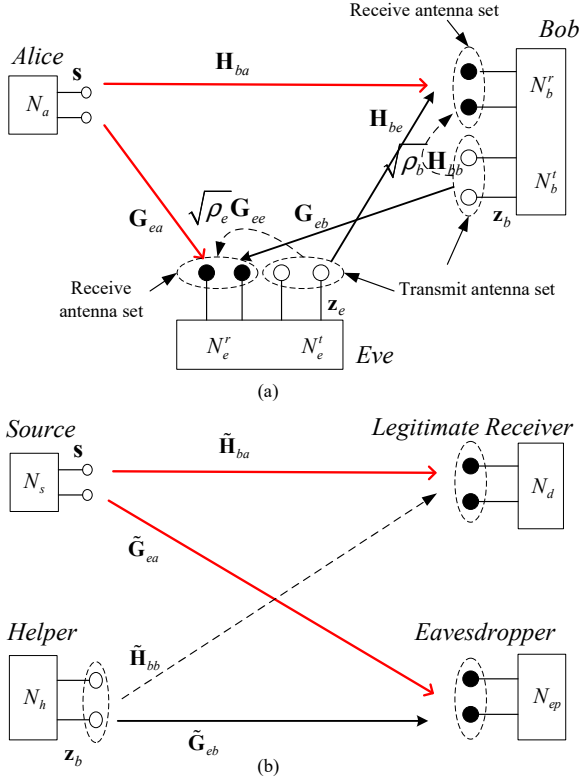


Fig. 1: (a) Gaussian wiretap channel with an active eavesdropper. (b) Helper-assisted Gaussian wiretap channel with a passive eavesdropper.

In Section IV, we consider an active *Eve* who knows the transmission strategy adopted by the legitimate terminals and tries to minimize the achievable S.D.o.F. by antenna allocation; for that case, we find the worst-case achievable S.D.o.F. Numerical results are given in Section V and conclusions are drawn in Section VI.

*Notation:*  $x \sim \mathcal{CN}(0, \Sigma)$  means  $x$  is a random variable following a complex circular Gaussian distribution with mean zero and covariance  $\Sigma$ ;  $(a)^+ \triangleq \max(a, 0)$ ;  $\lfloor a \rfloor$  denotes the biggest integer which is less or equal to  $a$ ;  $|a|$  denotes the absolute value of  $a$ . We use lower case bold to denote vectors;  $\mathbf{I}$  represents an identity matrix with appropriate size;  $\mathbb{C}^{N \times M}$  indicates a  $N \times M$  complex matrix set;  $\mathbf{A}^H$ ,  $\text{tr}\{\mathbf{A}\}$ ,  $\text{rank}\{\mathbf{A}\}$ , and  $|\mathbf{A}|$  stand for the hermitian transpose, trace, rank and determinant of the matrix  $\mathbf{A}$ , respectively.

## II. SYSTEM MODEL AND PROBLEM STATEMENT

We consider a Gaussian wiretap channel (see Fig. 1(a)) consisting of *Alice*, *Bob*, and *Eve*, equipped with  $N_a$ ,  $N_b$  and  $N_e$  antennas, respectively. *Eve* is an active agent, who works in FD mode, i.e., it allocates  $N_e^r$  antennas to receive signals and uses the remaining  $N_e^t = N_e - N_e^r$  antennas to transmit isotropic noise, i.e.,  $\mathbf{z}_e$ , with  $E\{\mathbf{z}_e \mathbf{z}_e^H\} = (P/N_e^t)\mathbf{I}$ . *Alice* wishes to send message  $\mathbf{s} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$  to *Bob* and keep it secret from *Eve*. Towards that objective, *Bob* allocates  $N_b^r$  antennas to receive the message and uses the remaining  $N_b^t = N_b - N_b^r$  antennas to transmit jamming signals, i.e.,  $\mathbf{z}_b$ , with  $\mathbf{z}_b \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ . Since *Bob* transmits noise while receiving the signal of interest, he generates self-interference, and so does

*Eve*. While several self-interference cancellation techniques have been reported, such as antenna isolation, analog-circuit-domain based methods and digital-domain based methods, full self-interference cancellation is still not achievable [24]. To describe the effect of residual self-interference we employ the loop interference model of [12], which quantifies the level of self-interference with a parameter  $\rho \in [0, 1]$ , with  $\rho = 0$  denoting zero self-interference.

To improve the system performance, *Alice* and *Bob* will precode their transmissions, using precoding matrices  $\mathbf{V}_a$  and  $\mathbf{V}_b$ , respectively. The signal received at *Bob* and *Eve* can be respectively written as

$$\mathbf{y}_b = \mathbf{H}_{ba} \mathbf{V}_a \mathbf{s} + \sqrt{\rho_b} \mathbf{H}_{bb} \mathbf{V}_b \mathbf{z}_b + \mathbf{H}_{be} \mathbf{z}_e + \mathbf{n}_b, \quad (1)$$

$$\mathbf{y}_e = \mathbf{G}_{ea} \mathbf{V}_a \mathbf{s} + \mathbf{G}_{eb} \mathbf{V}_b \mathbf{z}_b + \sqrt{\rho_e} \mathbf{G}_{ee} \mathbf{z}_e + \mathbf{n}_e, \quad (2)$$

where  $\mathbf{n}_b \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$  and  $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$  represent additive white Gaussian noise (AWGN) vectors at *Bob* and *Eve*, respectively;  $\mathbf{H}_{ba} \in \mathbb{C}^{N_b^r \times N_a}$  and  $\mathbf{H}_{be} \in \mathbb{C}^{N_e^r \times N_a}$  denote the channel matrices from *Alice* and *Eve* to *Bob*, respectively;  $\mathbf{G}_{ea} \in \mathbb{C}^{N_e^r \times N_a}$  and  $\mathbf{G}_{eb} \in \mathbb{C}^{N_e^r \times N_b^t}$  denote the channel matrices from *Alice* and *Bob* to *Eve*, respectively;  $\mathbf{H}_{bb} \in \mathbb{C}^{N_b^r \times N_b^t}$  and  $\mathbf{G}_{ee} \in \mathbb{C}^{N_e^r \times N_e^t}$  represent the self-interference channel matrices at *Bob* and *Eve*, respectively;  $\rho_b$  and  $\rho_e$  denote the self-interference level of *Bob* and *Eve*, respectively. The transmitted signals including the message signal  $\mathbf{s}$  and the jamming signals  $\mathbf{z}_b$  and  $\mathbf{z}_e$  are independent of each other, and independent of the noise  $\mathbf{n}_b$  and  $\mathbf{n}_e$ . Since *Alice* and *Bob* are not expected to cooperate with *Eve*, *Eve* cannot do any precoding. The only way *Eve* can affect the achievable S.D.o.F. is by optimizing its transmit/receive antenna allocation.

In the above, the Gaussian signaling assumption is made in order to maximize the achievable secrecy transmission rate [25], [26]. Also, the flat fading assumption used in (1), (2) is valid when the coherence bandwidth of the channel is larger than the bandwidth of the transmitted signal [27]. Here we assume that all channels are known at the legitimate nodes, including the CSI for *Eve*. This is possible in situations in which *Eve* is an active network user and its whereabouts and behavior can be monitored.

For a given precoding matrix pair  $(\mathbf{V}_a, \mathbf{V}_b)$ , the maximum achievable rate at *Bob* and *Eve* can be respectively expressed as [28]

$$R_b = \log |\mathbf{I} + (\mathbf{I} + \mathbf{W}_b)^{-1} \mathbf{H}_{ba} \mathbf{Q}_a \mathbf{H}_{ba}^H|, \quad (3a)$$

$$R_e = \log |\mathbf{I} + (\mathbf{I} + \mathbf{W}_e)^{-1} \mathbf{G}_{ea} \mathbf{Q}_a \mathbf{G}_{ea}^H|, \quad (3b)$$

where  $\mathbf{Q}_a \triangleq \mathbf{V}_a \mathbf{V}_a^H$  and  $\mathbf{Q}_b \triangleq \mathbf{V}_b \mathbf{V}_b^H$  denote the input covariance matrices at *Alice* and *Bob*, respectively, with the average transmit power budget  $\text{tr}\{\mathbf{Q}_a\} = \text{tr}\{\mathbf{Q}_b\} = P$ ; the interference covariance matrices at *Bob* and *Eve* respectively are

$$\mathbf{W}_b \triangleq \rho_b \mathbf{H}_{bb} \mathbf{Q}_b \mathbf{H}_{bb}^H + \frac{P}{N_e^t} \mathbf{H}_{be} \mathbf{H}_{be}^H,$$

$$\mathbf{W}_e \triangleq \mathbf{G}_{eb} \mathbf{Q}_b \mathbf{G}_{eb}^H + \frac{\rho_e P}{N_e^t} \mathbf{G}_{ee} \mathbf{G}_{ee}^H.$$

Correspondingly, the achievable S.D.o.F., representing the high SNR behavior of the achievable secrecy rate [29], is

$$d_{s,a}(\mathbf{Q}_a, \mathbf{Q}_b) \triangleq \lim_{P \rightarrow \infty} \frac{R_b - R_e}{\log P}, \quad (4)$$

provided that a positive secrecy rate can be achieved.

The goal of this paper is to determine the maximum achievable S.D.o.F. over the transmission schemes at *Alice* and *Bob*, i.e., the antenna allocation at *Bob* and the precoding matrices of *Alice* and *Bob*. To that goal, in the following, we will first determine the optimal number of transmit/receive antennas at *Bob*, based on which we then analytically determine the maximum achievable S.D.o.F.. Subsequently, we find the worst-case achievable S.D.o.F. for the adverse scenario, in which *Eve* is smart and tries to minimize the achievable S.D.o.F. by adjusting the number of transmit/receive antennas.

### III. THE MAXIMUM ACHIEVABLE S.D.O.F.

In [30], [31], we determined the maximum achievable S.D.o.F. for a helper-assisted Gaussian wiretap channel, which consists of a source equipped with  $N_s$  antennas, a legitimate receiver equipped with  $N_d$  antennas, a passive eavesdropper equipped with  $N_{ep}$  antennas, and an external helper (sending jamming signals to confuse *Eve*) equipped with  $N_h$  antennas. In that scenario, the main idea for achieving the maximum S.D.o.F. is to include into the source and helper precoding matrix pair the maximum possible linearly precoding vector pairs along which the message and jamming signals are aligned into the same received subspace of *Eve*, subject to the constraint that the total number of signal streams *Bob* can see is no greater than its total number of receive antennas. The achievable S.D.o.F. equals the number of precoding vectors that has been included into the source precoding matrix. For easy reference the helper-assisted Gaussian wiretap channel studied in [30] is depicted in Fig. 1(b). As we will show next, the maximum achievable S.D.o.F. of the wiretap channel of Fig. 1(a) is equal to that of the wiretap channel of Fig. 1(b) with parameters as given in the following proposition.

**Proposition 1:** *Provided that  $N_e^t < \min\{N_b^r, N_e^r\}$ , the maximum achievable S.D.o.F. of the MIMO Gaussian wiretap channel of Fig. 1(a), is equal to that of a helper-assisted wiretap channel of Fig. 1(b), with  $N_s = N_a$ ,  $N_h = N_b^t$ ,  $N_d = N_b^r - N_e^t$  and  $N_{ep} = N_e^r - N_e^t$ .*

*Proof:* See Appendix A. ■

**Remark 1:** Based on Proposition 1, one can see that if  $N_e^t < \min\{N_b^r, N_e^r\}$  the maximum S.D.o.F. of the system under consideration can be determined based on results on the helper-assisted wiretap channel. Otherwise, if  $N_e^t \geq N_b^r$  and independent of  $N_e^r$ , the maximum achievable S.D.o.F. is zero, since *Bob* already cannot see any interference-free subspaces; if  $N_e^t \geq N_e^r$ , *Eve* cannot see any interference-free subspaces, and so the maximum achievable S.D.o.F. is equal to  $\min\{(N_b^r - N_e^t)^+, N_a\}$ . Therefore, for the purpose of computing the maximum achievable S.D.o.F. of the system under consideration, we only need to investigate that of the corresponding helper-assisted wiretap channel.

Next, we show that for a fixed total number of helper and destination antennas, i.e.,  $N_h + N_d = N_{\text{sum}}$ , one can find a

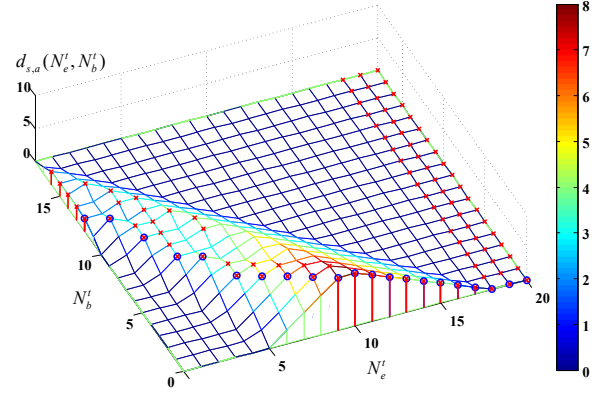


Fig. 2: The maximum achievable S.D.o.F. for the system with  $N_a = 10$ ,  $N_b = 18$  and  $N_e = 20$ .

solution for the number of helper antennas which achieves the maximum S.D.o.F.. Details are given in the following proposition.

**Proposition 2:** *Consider the helper-assisted wiretap channel of Fig. 1(b). Suppose that  $N_h$  and  $N_d$  can vary but their sum is always fixed at  $N_{\text{sum}}$ . Then, the maximum achievable S.D.o.F. is*

$$d_{s,p} = \min\{\delta, N_{\text{sum}}, N_s\}, \quad (5)$$

where  $\delta \triangleq \lfloor \frac{(N_{\text{sum}} - |N_s - N_{ep}|)^+}{3} \rfloor + (N_s - N_{ep})^+$ .

- 1) If  $N_{\text{sum}} \leq N_{ep} - N_s$ , the maximum achievable S.D.o.F. is zero for any pair of  $(N_h, N_d)$ .
- 2) If  $N_{\text{sum}} \leq N_s - N_{ep}$ , the maximum S.D.o.F. is achieved when  $N_d = N_{\text{sum}}$  with no antennas being allocated to the helper.
- 3) If  $N_{\text{sum}} > |N_s - N_{ep}|$ , the maximum S.D.o.F. is achieved when  $N_h = \hat{N}_h$ , where

$$\hat{N}_h = \begin{cases} N_{ep} - N_s + \lfloor \frac{N_{\text{sum}} - |N_s - N_{ep}|}{3} \rfloor & \text{if } N_s \leq N_{ep}, \\ \lfloor \frac{N_{\text{sum}} - |N_s - N_{ep}|}{3} \rfloor & \text{if } N_s > N_{ep}, \end{cases}$$

and the remaining  $N_{\text{sum}} - \hat{N}_h$  antennas are assigned to the legitimate receiver.

*Proof:* See Appendix B. ■

Combining Proposition 1 and Proposition 2, we can determine the maximum achievable S.D.o.F. for the system under consideration as follows.

**Theorem 1:** *Consider a MIMO Gaussian wiretap channel, as depicted in Fig. 1(a). The maximum achievable S.D.o.F. is*

$$d_{s,a}(N_e^t) = \begin{cases} \min\{(N_b - N_e^t)^+, N_a\} & \text{if } N_e^t \geq N_e^r, \\ \min\{\eta, (N_b - N_e^t)^+, N_a\} & \text{if } N_e^t < N_e^r, \end{cases} \quad (6)$$

with  $\eta \triangleq \lfloor \frac{(N_b - N_e^t - |N_a - N_e^r + N_e^t|)^+}{3} \rfloor + (N_a - N_e^r + N_e^t)^+$ . The maximum S.D.o.F. is achieved when *Bob* uses  $N_b^{t*}$  antennas to transmit, with  $N_b^{t*}$  given in (7) at the top of the next page, and the remaining  $N_b - N_b^{t*}$  antennas receive.

*Proof:* See Appendix C. ■

Theorem 1 provides the number of transmit antennas at *Bob* which achieves the maximum S.D.o.F.. This is illustrated in Fig. 2, where we plot the maximum achievable S.D.o.F. for the system with  $N_a = 10$ ,  $N_b = 18$  and  $N_e = 20$ . Specifically, for a given antenna number pair  $(N_e^t, N_b^t)$ , we

$$N_b^{t*} = \begin{cases} N_e^r - N_e^t - N_a + \lfloor \frac{N_b - N_e^t - |N_a - N_e^r + N_e^t|}{3} \rfloor & \text{if } N_e^t < \min\{N_e^r, N_b - |N_a - N_e^r + N_e^t|\} \text{ and } N_a \leq N_e^r - N_e^t \\ \lfloor \frac{N_b - N_e^t - |N_a - N_e^r + N_e^t|}{3} \rfloor & \text{if } N_e^t < \min\{N_e^r, N_b - |N_a - N_e^r + N_e^t|\} \text{ and } N_a > N_e^r - N_e^t \\ 0 & \text{otherwise} \end{cases} \quad (7)$$

plot the achievable S.D.o.F. based on *Remark 1*. For each fixed  $N_e^t$ , we find, with the numerical search method, the points which achieve the maximum S.D.o.F., and mark them with red crosses. Looking at the slice of the graph corresponding to a fixed  $N_e^t$ , one can see that there are one or more  $N_b^{t*}$ 's which achieve the maximum S.D.o.F., and  $N_b^{t*}$  marked by a blue circle, coincides with one of those red crosses.

#### A. The proposed transmission scheme which achieves the maximum S.D.o.F.

With the optimal allocation of transmit/receive antennas at *Bob*, we next construct the pair  $(\mathbf{V}_a^*, \mathbf{V}_b^*)$  which achieves the maximum S.D.o.F..

- 1) For the case of  $N_b^{t*} = 0$ , and along the lines of Appendix A, one can see that the wiretap channel of Fig. 1(a) is equivalent to a classic three-node wiretap channel, with the main channel and eavesdropping channel being equal to  $\mathbf{U}_b^{0H} \mathbf{H}_{ba}$  and  $\mathbf{U}_e^{0H} \mathbf{G}_{ea}$ , respectively. Here,  $\mathbf{U}_b^0$  and  $\mathbf{U}_e^0$  are the orthonormal basis of the null space of  $\mathbf{H}_{be}$  and  $\mathbf{G}_{ee}$ , respectively. Therefore, by applying the precoding matrix design of the three-node wiretap channel of [3], the maximum S.D.o.F. can be achieved. According to [3], the precoding matrices are constructed by selecting those linearly independent precoding vectors along which the legitimate channel has better quality than the eavesdropping channel.
- 2) For the case of  $N_b^{t*} \neq 0$ , and along the lines of Appendix A, one can see that the wiretap channel of Fig. 1(a) is equivalent to a classic helper-assisted wiretap channel, with the channels to *Bob* being equal to  $\mathbf{U}_b^{0H} \mathbf{H}_{ba}$  and  $\mathbf{U}_b^{0H} \mathbf{H}_{bb}$ , the channels to *Eve* being equal to  $\mathbf{U}_e^{0H} \mathbf{G}_{ea}$  and  $\mathbf{U}_e^{0H} \mathbf{G}_{eb}$ , and the number of antennas being  $N_s = N_a$ ,  $N_h = N_b^t$ ,  $N_d = N_b^r - N_e^t$  and  $N_{ep} = N_e^r - N_e^t$ . Therefore, by applying the precoding matrix design of [30], [31] to this equivalent helper-assisted wiretap channel, the maximum S.D.o.F. can be achieved. The main idea here is to select the maximum possible number of linearly independent precoding vector pairs along which the message and jamming signals are aligned into the same received subspace of *Eve*. In particular, we divide the candidate set of precoding vector pairs into three subsets, i.e., C1, in which the message signal sent by *Alice* spreads within the null space of the eavesdropping channel, C2, in which the message does not spread within the null space of the eavesdropping channel and *Bob* is self-interference free, and C3, in which the message does not spread within the null space of the eavesdropping channel and *Bob* suffers from self-interference. We select precoding vector pairs

from C1 first, followed by C2 and then C3, until there are no more candidate precoding vector pairs or the total number of signal streams *Bob* can see is equal to its total number of receive antennas. For more details on determining the number of candidates of each subset and their formulas, please refer to [30], [31]. It is worth noting that (to be used in Section V) the formulas of the precoding vector pairs in C1 only depend on the channel matrix  $\mathbf{U}_e^{0H} \mathbf{G}_{ea}$ ; the formulas of the precoding vector pairs in C3 only depend on the channel matrices  $\mathbf{U}_e^{0H} \mathbf{G}_{ea}$  and  $\mathbf{U}_e^{0H} \mathbf{G}_{eb}$ ; in addition to  $\mathbf{U}_e^{0H} \mathbf{G}_{ea}$  and  $\mathbf{U}_e^{0H} \mathbf{G}_{eb}$ , the formulas of the precoding vector pairs in C2 also depend on the channel matrix  $\mathbf{U}_b^{0H} \mathbf{H}_{bb}$ .

#### IV. WORST-CASE ACHIEVABLE S.D.o.F. IN THE PRESENCE OF A SMART *Eve*

In this section, we consider a scenario in which *Eve* knows the transmit strategies at both *Alice* and *Bob*, and therefore it derives  $d_{s,a}(N_e^t)$ , based on which it adjusts the number of its transmit antennas in order to minimize the achievable S.D.o.F., i.e.,  $d_{s,a}(N_e^t)$ . In that case, the worst-case maximum achievable S.D.o.F. is

$$d_{s,a}^{\text{wc}} = \min_{0 \leq N_e^t \leq N_e} d_{s,a}(N_e^t). \quad (8)$$

*Theorem 2: Consider the MIMO Gaussian wiretap channel of Fig. 1(a). Assume that Eve knows the transmit strategies at Alice and Bob. Then, the maximum achievable S.D.o.F. is given in (9), which is shown at the top of next page.*

*Proof:* See Appendix D. ■

*Theorem 2* enables us to make some interesting observations, which are given in the following Corollaries.

*Corollary 1: For the purpose of minimizing the achievable S.D.o.F., Eve will jam or eavesdrop, but will not adopt a combination of both.*

*Proof:* From the proof of *Theorem 2* in Appendix D, one can see that the minimum value of  $d_{s,a}(N_e^t)$  is obtained only when  $N_e^t = 0$  or  $N_e^t = N_e$ . This completes the proof. ■

*Corollary 2: If  $N_b > N_e$ , a positive S.D.o.F. can always be achieved with the proposed cooperative transmission scheme.*

*Proof:* With the expression of (9), it can be verified that the worst-case achievable S.D.o.F. is greater than zero for the case of  $N_b > N_e$ . This completes the proof. ■

#### V. NUMERICAL RESULTS

As already mentioned, the achievable S.D.o.F. reveals the high SNR behavior of the achievable secrecy rate. In this section, we consider a more realistic SNR scenario, and demonstrate the secrecy rate performance of the proposed

$$d_{s,a}^{\text{wc}} = \begin{cases} 0 & \text{if } N_e \geq N_b, \\ \min\{\lfloor \frac{N_b - N_e + N_a}{3} \rfloor, N_b - N_e, N_a\} & \text{if } \max\{\frac{N_b - N_a}{2}, N_a\} \leq N_e < N_b, \\ \min\{\lfloor \frac{N_b - N_a + N_e}{3} \rfloor + N_a - N_e, N_b - N_e\} & \text{if } \frac{N_b - N_a}{2} \leq N_e < \min\{N_b, N_a\} \text{ and } N_e > N_a - N_b, \\ N_b - N_e & \text{if } \frac{N_b - N_a}{2} \leq N_e < \min\{N_b, N_a\} \text{ and } N_e \leq N_a - N_b, \\ N_a & \text{if } N_e < \min\{\frac{N_b - N_a}{2}, N_b\}. \end{cases} \quad (9)$$

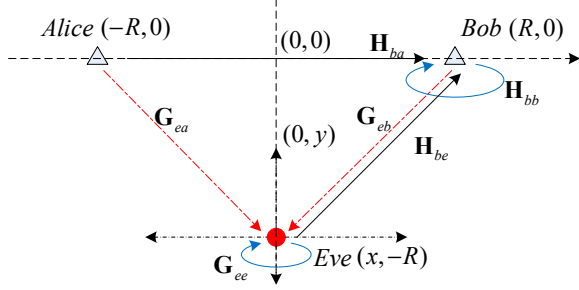


Fig. 3: Model used for numerical experiments.

approach. In particular, we consider a scenario as shown in Fig. 3. *Alice* and *Bob* are respectively fixed at coordinates  $(-R, 0)$  and  $(R, 0)$  (unit: meters). The smaller the  $R$ , the higher the received SNR at *Bob* will be. *Eve* can move in one of the following two ways, i.e., parallel to the  $x$ -axis and between the points  $(-20, -R)$  and  $(20, -R)$ , and parallel to the  $y$ -axis and between the points  $(0, 10)$  and  $(0, 0)$ .

Unless otherwise specified, we consider the strong self-interference level  $\rho_b = \rho_e = \rho = 1$ , and we set  $N_a = 4$ ,  $N_b = 7$ ,  $N_e^t = 1$  and  $N_e^r = 5$ . The transmit power of each node is  $P = 0\text{dBm}$ . The noise power level is set as  $\sigma^2 = -60\text{dBm}$ . The power is equally allocated between different signal streams at each node. According to *Theorem 1*, for the above system, the maximum achievable S.D.o.F. of 2 can be achieved by choosing  $N_b^t = 2$ ,  $N_b^r = 5$ . Setting  $N_b^t = 2$ ,  $N_b^r = 5$ , and according to Section III. A, one can see that the system under consideration is equivalent to the helper-assisted wiretap channel of Fig. 1(b), with the number of antennas being  $N_s = 4$ ,  $N_h = 2$ ,  $N_d = 4$  and  $N_{ep} = 4$ ; for that helper-assisted wiretap channel, the number of candidate precoding vector pairs in C1, C2 and C3 are respectively 0, 0 and 2. Following the construction method of Section III. A and since  $N_d = 4$  and for each precoding vector pair in C3 *Bob* suffers from self-interference, we can select two precoding vector pairs in C3 without violating the constraint that the total number of signal streams *Bob* can see is no greater than its total number of receive antennas. Therefore, a total of two precoding vector pairs can be picked, and as such a number of two message signal streams will be sent from *Alice*. We construct the precoding matrix pair assuming exact knowledge of the channels.

With the precoding matrix pair, we examine the achievable secrecy transmission rate, i.e.,  $(R_b - R_e)^+$ , where  $R_b$  and  $R_e$  are given by (3a) and (3b), respectively [28]. Results are obtained based on 1,000 Monte Carlo runs. In each run, the

effect of the channel on the transmitted signal is modeled by a multiplicative scalar of the form  $d^{-c/2}e^{j\theta}$  [32], where  $d$  is the distance between the transmit and receive terminals,  $c$  is the path loss exponent and  $\theta$  is a random phase, which is taken to be uniformly distributed within  $[0, 2\pi)$  and independent between runs. The value of  $c$  is typically in the range of 2 to 4. In our simulations we set  $c = 3.5$ . We assume that the distance of different combinations of transmit-receive antennas corresponding to the same link is the same, and as such the corresponding path loss is the same.

For comparison, we also plot the average achievable secrecy rate of the half-duplex (HD) scheme, wherein *Bob* receives with all of its antennas. For the HD scheme, the precoding matrix of *Alice* consists of the generalized eigenvectors corresponding to the largest two generalized eigenvalues of the matrix pair [3]

$$(\hat{\mathbf{H}}_{ba}^H(\mathbf{I} + \frac{P}{N_e^t}\hat{\mathbf{H}}_{be}\hat{\mathbf{H}}_{be}^H)^{-1}\hat{\mathbf{H}}_{ba}, \hat{\mathbf{G}}_{ea}^H(\mathbf{I} + \frac{\rho_e P}{N_e^t}\hat{\mathbf{G}}_{ee}\hat{\mathbf{G}}_{ee}^H)^{-1}\hat{\mathbf{G}}_{ea}), \quad (10)$$

where  $\hat{\mathbf{H}}_{ba}$  and  $\hat{\mathbf{H}}_{be}$  denote the channel matrices to *Bob*,  $\hat{\mathbf{G}}_{ea}$  and  $\hat{\mathbf{G}}_{ee}$  represent the channel matrices to *Eve*. From Section III. A, the proposed transmission scheme in terms of the achievable S.D.o.F. can be either equivalent with a three-node wiretap channel when  $N_b^{t*} = 0$ , or equivalent with a helper-assisted wiretap channel when  $N_b^{t*} \neq 0$ . In the former case, the proposed scheme reduces to an HD scheme. In the latter case, the proposed scheme always achieves a greater S.D.o.F. For comparison fairness, in the HD scheme we consider selecting the same number of message signal streams as in the proposed scheme.

Figs. 4 and 5 illustrate the average achievable secrecy transmission rate as function of *Eve*'s position, with the  $x$ -coordinate varying from  $-20$  to  $20$  and the  $y$ -coordinate fixed at  $-R$ . Fig. 4 corresponds to  $R = 10$ , which represents a low SNR scenario for *Bob*, while Fig. 5 corresponds to  $R = 1$ , which is a high SNR scenario for *Bob*. From Fig. 4, one can see that the proposed FD scheme performs overall better than the HD scheme, except when *Eve* is to the left of *Alice* or to the right of *Bob*. The behavior in the latter cases should be expected, since when *Eve* is to the left of *Alice*, the received jamming signal is too weak to disturb *Eve*'s channel. As a result, the HD scheme, which uses all of *Bob*'s antennas to receive, performs better. When *Eve* is to the right of *Bob*, the received SNR is already small even if *Bob* does not send jamming signals, and as a result, the HD scheme also performs better. Naturally, for the higher SNR case, the advantage of the



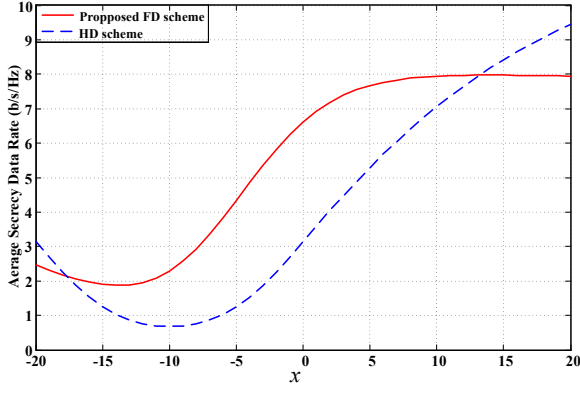


Fig. 4: Average achievable secrecy rate versus the position of *Eve* along the  $x$ -coordinate. The distance parameter  $R = 10$ .

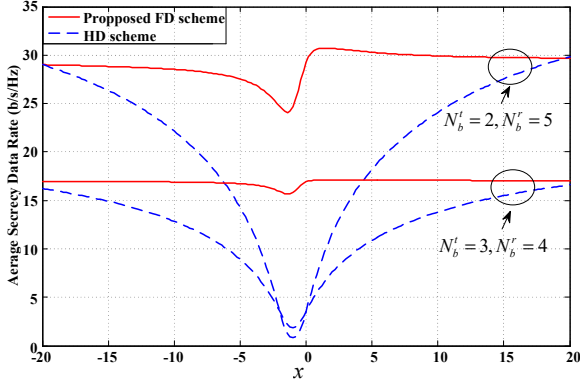


Fig. 5: Average achievable secrecy rate versus the position of *Eve* along the  $x$ -coordinate. The distance parameter  $R = 1$ .

proposed FD approach is bigger and evident over the entire range (see Fig. 5). To illustrate the secrecy rate advantage of using the proposed antenna allocation at *Bob*, i.e.,  $N_b^t = 2$  and  $N_b^r = 5$ , in Fig. 5 we also plot the achievable secrecy transmission rate for another allocation, i.e.,  $N_b^t = 3$  and  $N_b^r = 4$ ; in that case and according to Section III. A, one can see that only an S.D.o.F. of 1 can be achieved. As expected, the achievable secrecy transmission rate of that latter case is almost half of the proposed case, for which an S.D.o.F. of 2 can be achieved.

In Fig. 6, we plot the average achievable secrecy transmission rate versus the position of *Eve* along the  $y$ -axis, for the case of  $R = 10$  and  $R = 5$ . The figure shows that for both cases, the achievable secrecy transmission rate of the proposed FD scheme remains constant for all positions of *Eve*. In contrast, the achievable secrecy transmission rate of the HD scheme decreases as  $y$  approaches zero. This can be explained as follows. As *Eve* comes closer to *Alice*, it receives a stronger signal, and as a result the secrecy rate of the HD scheme decreases. On the other hand, in the proposed FD scheme, the message signal sent by *Alice* and the jamming signal sent by *Bob* are aligned into the same received subspace of *Eve*, thus keeping *Eve*'s eavesdropping capability constant, and as a result, keeping the achievable secrecy rate of the proposed FD scheme constant.

Fig. 7 illustrates the average achievable secrecy transmission rate of the proposed scheme as function of the self-

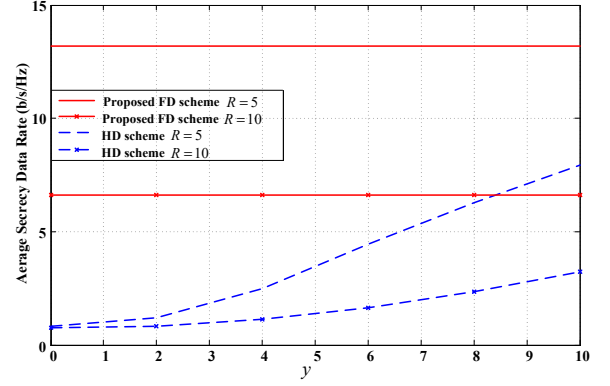


Fig. 6: Average achievable secrecy rate versus the position of *Eve* along the  $y$ -coordinate.

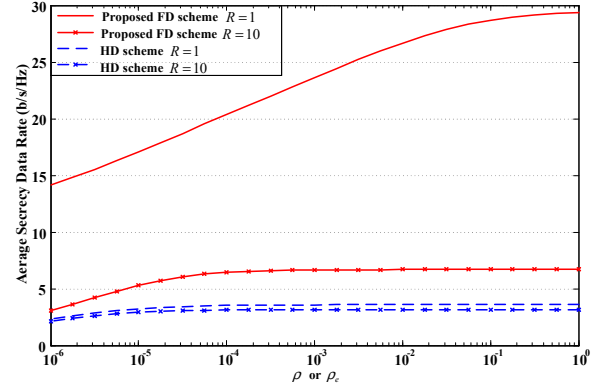


Fig. 7: Average achievable secrecy rate versus the self-interference level.

interference level  $\rho$ , and that of the HD scheme as function of the self-interference level  $\rho_e$ , for the case of  $R = 10$  and  $R = 1$ . We should note that since for the HD scheme *Alice* determines its precoding matrix with (10), the achievable secrecy transmission rate only relates to  $\rho_e$ . One can see that the achievable secrecy rate of the FD scheme increases as  $\rho$  increases. This is because, by aligning the message and jamming signals into the same received subspace of *Eve*, the proposed scheme delivers a distorted message signal to *Eve*, which makes the eavesdropping channel more sensitive to self-interference. Therefore, the achievable secrecy rate of the FD scheme increases with increasing level of self-interference. While the achievable secrecy rate of the HD scheme also increases with increasing level of the self-interference at *Eve*, the increase is small as compared to the proposed scheme.

In order to separately check the effect of the self-interference level, i.e.,  $\rho_b$  or  $\rho_e$ , on the achievable secrecy rate performance of the proposed scheme, in Fig. 8, we set  $\rho_e = 10^{-3}$  and plot the average achievable secrecy transmission rate versus the self-interference level  $\rho_b$ ; also, we set  $\rho_b = 10^{-3}$  and plot the average achievable secrecy transmission rate versus the self-interference level  $\rho_e$ . One can see that the achievable secrecy transmission rate decreases slightly with  $\rho_b$ , while it increases drastically with  $\rho_e$ . This can also be explained by the fact that, for the FD scheme the eavesdropping channel is more sensitive to self-interference.

In practice, perfect channel estimates are difficult to obtain.

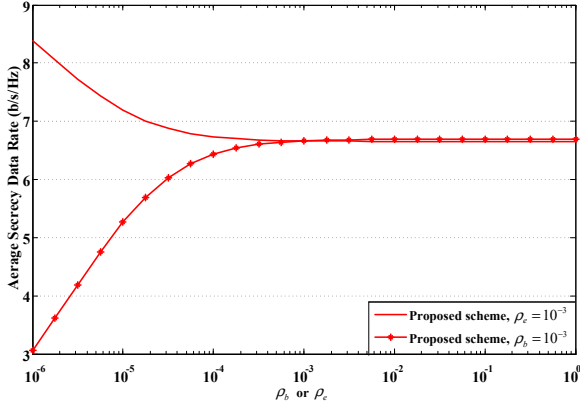


Fig. 8: Average achievable secrecy rate versus the self-interference level. The distance parameter  $R = 10$ .

Since the proposed precoding matrix design highly depends on the channels, we next examine the secrecy rate performance in the presence of imperfect channel estimates. We model imperfect CSI through a Gauss-Markov uncertainty of the form [33]

$$\mathbf{G}_{ei} = d_{ei}^{-c/2} \left( \sqrt{1 - \alpha^2} \bar{\mathbf{G}}_{ei} + \alpha \Delta \bar{\mathbf{G}}_{ei} \right), i = a, b, \quad (11)$$

where  $0 \leq \alpha \leq 1$  denotes the channel uncertainty.  $\alpha = 0$  and  $\alpha = 1$  correspond to perfect channel knowledge and no CSI knowledge, respectively. The entries of  $\bar{\mathbf{G}}_{ei}$  are  $e^{j\theta}$  with  $\theta$  be a random phase uniformly distributed within  $[0, 2\pi)$ .  $\Delta \bar{\mathbf{G}}_{ei} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$  represents the Gaussian error channel matrices.  $d_{ei}$  denotes the distance from *Alice* or *Bob*. With the same channel model as in (11), we model the channel uncertainty of the channels  $\mathbf{H}_{bi}$ ,  $i = a, b, e$ . We construct the precoding matrix pair  $(\mathbf{V}_a, \mathbf{V}_b)$  with the estimated channels.

In Fig. 9, we plot the achievable secrecy rate with respect to the channel uncertainty in  $\mathbf{H}_{bi}$ ,  $i = a, b, e$ , for the proposed antenna allocation scheme, i.e.,  $N_b^t = 2$ ,  $N_b^r = 5$ . It can be observed that the achievable secrecy rate remains constant for different channel uncertainties of  $\mathbf{H}_{bi}$ ,  $i = a, b, e$ . This should be expected, since the constructed precoding matrix pair consists of two precoding vector pairs from C3, whose formulas only depend on the matrices  $\mathbf{U}_e^{0H} \mathbf{G}_{ea}$  and  $\mathbf{U}_e^{0H} \mathbf{G}_{eb}$ . Therefore, the channels  $\mathbf{H}_{bi}$ ,  $i = a, b, e$  do not enter in the construction of the precoding matrix pair. Indeed, for the equivalent helper-assisted wiretap channel with the antenna allocation given by *Proposition 2*, i.e.,  $\tilde{N}_h$ , it can be verified that there are no candidate precoding vector pairs in C2. Therefore, the achievable secrecy rate of proposed scheme is independent of the channel uncertainties of  $\mathbf{H}_{bi}$ ,  $i = a, b, e$ . As illustrated in Fig. 2, for a given fixed  $N_e^t$  there may be more than one  $N_b^t$ 's which can achieve the maximum S.D.o.F. Intuitively, those schemes achieving the same S.D.o.F. can also achieve the same secrecy rate performance, which, combined with the fact that the proposed schemes's achievable secrecy rate remains unchanged even when the channel estimates turns noisy, indicates that the proposed scheme will outperform the others. Next, with simulations we show that advantage of the proposed scheme. Let's take the antenna allocation, i.e.,  $N_b^t = 4$ ,  $N_b^r = 3$ , as an example. Substituting  $N_b^t = 4$ ,

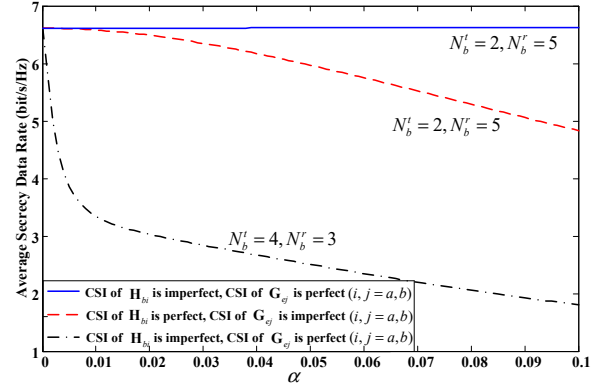


Fig. 9: Average achievable secrecy rate versus channel uncertainty. The distance parameter  $R = 10$ .

$N_b^r = 3$  into Section III. A, one can see that the maximum S.D.o.F. of 2 can also be achieved. In particular, with  $N_b^t = 4$ ,  $N_b^r = 3$  the system under consideration is equivalent to the helper-assisted wiretap channel of Fig. 1(b), with the number of antennas being  $N_s = 4$ ,  $N_h = 4$ ,  $N_d = 2$  and  $N_{ep} = 4$ ; for that helper-assisted wiretap channel, the number of candidate precoding vector pairs in C1, C2 and C3 are respectively 0, 2 and 2. Following the construction method in Section III. A, we first select the two candidate precoding vector pairs in C2. Since  $N_d = 2$ , we cannot pick any more precoding vector pairs without violating the constraint that the total number of signal streams *Bob* can see is no greater than its total number of receive antennas. Concluding, a total of two precoding vector pairs can be picked from C2, and as such an S.D.o.F. of 2 can be achieved [30], [31]. Based on Fig. 9 one can see that the proposed scheme, i.e.,  $N_b^t = 2$ ,  $N_b^r = 5$ , and that with  $N_b^t = 4$ ,  $N_b^r = 3$ , provide the same secrecy rate performance when the channel estimates are perfect. Moreover, when the channel estimates are noisy, i.e.,  $\alpha > 0$ , the proposed scheme outperforms the other one, since the achievable secrecy rate of the proposed scheme remains unchanged while that of the other scheme drops with the increase of uncertainty in the channels  $\mathbf{H}_{bi}$ ,  $i = a, b, e$ . This is because, unlike the proposed scheme the formulas of the precoding vector pairs of the other one are from C2, and as such they depend on the channel  $\mathbf{U}_b^{0H} \mathbf{H}_{bb}$ .

On the other hand, in Fig. 9 it can be observed that the achievable secrecy rate drops with the increase of uncertainty in the channels  $\mathbf{G}_{bi}$ ,  $i = a, b, e$ . This should be expected, since the benefits brought by the proposed scheme come from the successful alignment of the message and jamming signals at *Eve*. To achieve that goal, the exact knowledge of the channels  $\mathbf{G}_{ei}$ ,  $i = a, b, e$ , is necessary. As a conclusion, one can see that the uncertainty in the channels  $\mathbf{G}_{ei}$ ,  $i = a, b, e$ , is more dangerous.

## VI. CONCLUSION

We have analytically addressed the S.D.o.F. maximization problem of a MIMO Gaussian wiretap channel in the presence of an active *Eve*. Specifically, we have proposed a Full-Duplex *Bob* scheme, where *Bob* divides the antenna set into two parts, one devoted to receiving and the other to jamming. Based on

the proposed scheme, we have derived the optimal number of transmit/receive antennas at *Bob*, and determined the maximum S.D.o.F., as a function of the number of antennas at each terminal. We have further found the worst-case achievable S.D.o.F. for the adverse scenario in which *Eve* knows the transmit strategies and tries to minimize the S.D.o.F. by adjusting its number of transmit/receive antennas. Our analysis has revealed that a positive S.D.o.F. can be guaranteed as long as it holds that  $N_b > N_e$ . We have also constructed a precoding matrix pair which achieves the maximum S.D.o.F. Numerical results have revealed the advantages of the proposed secrecy transmission scheme over the existing half-duplex scheme, and have validated the robustness of the proposed scheme under realistic scenarios.

#### APPENDIX A PROOF OF Proposition 1

Given an arbitrary point  $(\mathbf{V}_a, \mathbf{V}_b)$ , with  $\text{tr}\{\mathbf{Q}_a\} = P$  and  $\text{tr}\{\mathbf{Q}_b\} = P$ . We can respectively rewrite  $\mathbf{Q}_a$  and  $\mathbf{Q}_b$  as  $\mathbf{Q}_a = P\bar{\mathbf{Q}}_a$  and  $\mathbf{Q}_b = P\bar{\mathbf{Q}}_b$ , with  $\text{tr}\{\bar{\mathbf{Q}}_a\} = \text{tr}\{\bar{\mathbf{Q}}_b\} = 1$ . Correspondingly, (3a) can be rewritten as

$$R_b = I_b^2 - I_b^1, \quad (12)$$

where

$$I_b^1 \triangleq \log|\mathbf{I} + P\mathbf{M}\mathbf{H}_{bb}\bar{\mathbf{Q}}_b\mathbf{H}_{bb}^H|, \quad (13a)$$

$$I_b^2 \triangleq \log|\mathbf{I} + P\mathbf{M}(\mathbf{H}_{bb}\bar{\mathbf{Q}}_b\mathbf{H}_{bb}^H + \mathbf{H}_{ba}\bar{\mathbf{Q}}_a\mathbf{H}_{ba}^H)|, \quad (13b)$$

with  $\mathbf{M} \triangleq (\mathbf{I} + \frac{P}{N_e^t}\mathbf{H}_{be}\mathbf{H}_{be}^H)^{-1}$ .

Let  $\mathbf{H}_{be}\mathbf{H}_{be}^H = [\mathbf{U}_b^1 \mathbf{U}_b^0] \begin{bmatrix} \Sigma_b & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{U}_b^{1H} \\ \mathbf{U}_b^{0H} \end{bmatrix}$  be the singular value decomposition (SVD), and then

$$\mathbf{M} = \mathbf{U}_b^1(\mathbf{I} + \frac{P}{N_e^t}\Sigma_b)^{-1}\mathbf{U}_b^{1H} + \mathbf{U}_b^0\mathbf{U}_b^{0H}. \quad (14)$$

Substituting (14) into (13a) and (13b), respectively, we obtain

$$\lim_{P \rightarrow \infty} \frac{I_b^1}{\log(P)} = \lim_{P \rightarrow \infty} \frac{\log|\mathbf{I} + P\bar{\mathbf{H}}_{bb}\bar{\mathbf{Q}}_b\bar{\mathbf{H}}_{bb}^H|}{\log(P)}, \quad (15a)$$

$$\lim_{P \rightarrow \infty} \frac{I_b^2}{\log(P)} = \lim_{P \rightarrow \infty} \frac{\log|\mathbf{I} + P(\bar{\mathbf{H}}_{bb}\bar{\mathbf{Q}}_b\bar{\mathbf{H}}_{bb}^H + \bar{\mathbf{H}}_{ba}\bar{\mathbf{Q}}_a\bar{\mathbf{H}}_{ba}^H)|}{\log(P)}, \quad (15b)$$

where  $\bar{\mathbf{H}}_{bb} \triangleq \mathbf{U}_b^{0H}\mathbf{H}_{bb}$ ,  $\bar{\mathbf{H}}_{ba} \triangleq \mathbf{U}_b^{0H}\mathbf{H}_{ba}$ .

Combining (12), (15a) and (15b), we arrive at that

$$\lim_{P \rightarrow \infty} \frac{R_b}{\log(P)} = \lim_{P \rightarrow \infty} \frac{\log|\mathbf{I} + (\mathbf{I} + P\bar{\mathbf{H}}_{bb}\bar{\mathbf{Q}}_b\bar{\mathbf{H}}_{bb}^H)^{-1}P\bar{\mathbf{H}}_{ba}\bar{\mathbf{Q}}_a\bar{\mathbf{H}}_{ba}^H|}{\log(P)}. \quad (16)$$

Letting  $\mathbf{G}_{ee}\mathbf{G}_{ee}^H = [\mathbf{U}_e^1 \mathbf{U}_e^0] \begin{bmatrix} \Sigma_e & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{U}_e^{1H} \\ \mathbf{U}_e^{0H} \end{bmatrix}$  be the SVD, and applying the same derivations from (12) to (16), we obtain that

$$\lim_{P \rightarrow \infty} \frac{R_e}{\log(P)} = \lim_{P \rightarrow \infty} \frac{\log|\mathbf{I} + (\mathbf{I} + P\bar{\mathbf{G}}_{eb}\bar{\mathbf{Q}}_b\bar{\mathbf{G}}_{eb}^H)^{-1}P\bar{\mathbf{G}}_{ea}\bar{\mathbf{Q}}_a\bar{\mathbf{G}}_{ea}^H|}{\log(P)}, \quad (17)$$

where  $\bar{\mathbf{G}}_{ea} \triangleq \mathbf{U}_e^{0H}\mathbf{G}_{ea}$  and  $\bar{\mathbf{G}}_{eb} \triangleq \mathbf{U}_e^{0H}\mathbf{G}_{eb}$ .

Combining (16) and (17), one can see that the achievable S.D.o.F. is equal to that of a helper-assisted wiretap channel,

with the channels to *Bob* as  $\mathbf{U}_b^{0H}\mathbf{H}_{ba}$  and  $\mathbf{U}_b^{0H}\mathbf{H}_{bb}$ , and the channels to *Eve* as  $\mathbf{U}_e^{0H}\mathbf{G}_{ea}$  and  $\mathbf{U}_e^{0H}\mathbf{G}_{eb}$ , respectively. Since  $N_e^t < N_b^r$  and  $N_e^t < N_e^r$ , and all the channel matrices are assumed to be full rank, this helper-assisted wiretap channel has effective number of antennas  $N_s = N_a$ ,  $N_h = N_b^t$ ,  $N_d = N_b^r - N_e^t$  and  $N_{ep} = N_e^r - N_e^t$ . This completes the proof.

#### APPENDIX B PROOF OF Proposition 2

It can be verified that, for the case of  $N_{\text{sum}} \leq N_s - N_{ep}$ , the maximum achievable S.D.o.F. equals  $N_{\text{sum}}$ , which is consistent with (5); for the case of  $N_{\text{sum}} \leq N_{ep} - N_s$ , the maximum achievable S.D.o.F. equals 0, which is also consistent with (5). Thus, in the sequel, we only need to focus on the case of  $N_{\text{sum}} > |N_s - N_{ep}|$ , in which

$$d_{s,p} = \min\{\delta, N_{\text{sum}}, N_s\}, \quad (18)$$

where  $\delta = \lfloor \frac{N_{\text{sum}} - |N_s - N_{ep}|}{3} \rfloor + (N_s - N_{ep})^+$ .

According to *Theorem 1* of [30] or equation (36) of [31], the maximum achievable S.D.o.F. for such a helper-assisted wiretap channel is

$$g(N_h) = \min\{d_{c=1}(N_h) + d_{c=2}^*(N_h), N_d, N_s\}, \quad (19)$$

where

$$d_{c=1}(N_h) \triangleq (N_s - N_{ep})^+ + s_1(N_h), \quad (20a)$$

$$d_{c=2}^*(N_h) \triangleq \min\{s_2(N_h), \lfloor (N_d - d_{c=1}(N_h))^+ / 2 \rfloor\}, \quad (20b)$$

with

$$s_1(N_h) \triangleq (\min\{N_s, N_{ep}\} + \min\{(N_h - N_d)^+, N_{ep}\} - N_{ep})^+,$$

$$s_2(N_h) \triangleq (\min\{N_s, N_{ep}\} + \min\{N_h, N_{ep}\} - N_{ep})^+ - s_1(N_h).$$

In the following, we will consider two distinct cases, i.e., the case of  $N_s \leq N_{ep}$  and the case of  $N_s > N_{ep}$ . For each case we first give a specific value of  $N_h$ , denoted by  $\hat{N}_h$ , which satisfies  $g(\hat{N}_h) = d_{s,p}$ . We then prove that for any  $N_h \neq \hat{N}_h$ , it holds that  $g(N_h) \leq d_{s,p}$ . In this way, we complete the proof of *Proposition 2*.

A. For the case of  $N_s \leq N_{ep}$

It holds that  $\delta = \lfloor \frac{N_{\text{sum}} - |N_s - N_{ep}|}{3} \rfloor$ .

Let  $\hat{N}_d = 2\lfloor \frac{N_{\text{sum}} - |N_s - N_{ep}|}{3} \rfloor + i$ , and

$$\hat{N}_h = \lfloor \frac{N_{\text{sum}} - |N_s - N_{ep}|}{3} \rfloor + (N_{ep} - N_s), \quad (21)$$

where  $i \triangleq N_{\text{sum}} - 3\bar{N}_d$ . By definition  $i \in \{0, 1, 2\}$ .

A. 1 When  $\delta \geq N_s$

In this subcase, it can be verified that  $N_{\text{sum}} \geq N_s$ . Thus, (18) becomes

$$d_{s,p} = N_s. \quad (22)$$

On the other hand, since  $\hat{N}_h \geq N_{ep}$ , (20a) becomes

$$d_{c=1}(\hat{N}_h) = N_s. \quad (23)$$



Substituting (23) into (19) and combined with the fact that  $\min\{\hat{N}_d, N_s\} = N_s$ , we arrive at  $g(\hat{N}_h) = N_s$ . Besides, by (19) the inequality  $g(N_h) \leq N_s$  always holds true. Therefore, the maximum value of  $g(N_h)$  over  $N_h$  is

$$g(\hat{N}_h) = N_s \stackrel{(a)}{=} d_{s,p},$$

where (a) comes from the equality in (22).

#### A. 2 When $\delta < N_s$

In this subcase, it can be verified that  $\delta < N_{\text{sum}}$ . Thus, (18) becomes

$$d_{s,p} = \delta. \quad (24)$$

On the other hand, since  $N_s \leq N_{ep}$  and  $\hat{N}_h - \bar{N}_d \leq N_{ep} - N_s$ , (20a) and (20b) respectively becomes

$$d_{c=1}(\hat{N}_h) = 0, \quad (25)$$

$$d_{c=2}^*(\hat{N}_h) = \delta. \quad (26)$$

Substituting (25) and (26) into (19) and combined with the fact that  $\min\{\delta, \hat{N}_d, N_s\} = \delta$ , we obtain

$$g(\hat{N}_h) = \delta \stackrel{(a)}{=} d_{s,p}, \quad (27)$$

where (a) comes from the equality in (24).

Next, we will prove that for any other  $N_h \neq \hat{N}_h$  it holds that  $g(N_h) \leq d_{s,p}$ , thus completing the proof that the maximum value of  $g(N_h)$  over  $N_h$  is  $g(\hat{N}_h) = d_{s,p}$ . To achieve that goal, we introduce  $\bar{N}_d = \lfloor \frac{N_{\text{sum}} - |N_s - N_{ep}|}{3} \rfloor$ , and

$$\bar{N}_h = 2 \lfloor \frac{N_{\text{sum}} - |N_s - N_{ep}|}{3} \rfloor + i + (N_{ep} - N_s).$$

With similar derivations from (22) to (27) it can be verified that  $g(\bar{N}_h) = d_{s,p} = g(\hat{N}_h)$ . In the remaining text of this subsection, we will show that for any other  $N_h \neq \bar{N}_h$  it holds that  $g(N_h) \leq d_{s,p}$ .

i) For any  $N_h > \bar{N}_h$ , it holds that  $N_d < \bar{N}_d$ . In addition, by (19) it holds that  $g(N_h) \leq N_d$ . Therefore,

$$g(N_h) < \bar{N}_d = d_{s,p}.$$

ii) For any  $N_h < \bar{N}_h$ , say  $N_h = \bar{N}_h - k$  with  $k \geq 1$ , i.e.,

$$\begin{aligned} N_h &= 2\bar{N}_d + i + (N_{ep} - N_s) - k, \\ N_d &= \bar{N}_d + k. \end{aligned}$$

Thus,  $N_h - N_d = \bar{N}_d + (N_{ep} - N_s) + i - 2k < N_{ep}$ , which, together with (20a), gives

$$d_{c=1}(N_h) = (\bar{N}_d + i - 2k)^+. \quad (28)$$

1) For the case of  $2k \leq \bar{N}_d + i$ , (28) becomes  $d_{c=1}(N_h) = \bar{N}_d + i - 2k$ , which, combined with (20b), gives  $d_{c=2}^*(N_h) \leq \lfloor \frac{3k-i}{2} \rfloor$ . Therefore,

$$\begin{aligned} g(N_h) &\leq d_{c=1}(N_h) + d_{c=2}^*(N_h) \\ &\leq \bar{N}_d + i - 2k + \lfloor \frac{3k-i}{2} \rfloor \\ &\stackrel{(a)}{\leq} \bar{N}_d \stackrel{(b)}{=} d_{s,p}. \end{aligned}$$

Here, since  $i \leq 2$  and  $k \geq 1$ , it holds true that  $i - 2k + \lfloor \frac{3k-i}{2} \rfloor \leq 0$ , and as a result, (a) holds true; (b) comes from the equality in (24).

2) For the case of  $\bar{N}_d + i < 2k \leq 2(\bar{N}_d + 1)$ , (28) becomes  $d_{c=1}(N_h) = 0$ . In addition, by (20b), it holds that  $d_{c=2}^*(N_h) \leq \lfloor N_d/2 \rfloor$ , which, combined with  $N_d = \bar{N}_d + k \leq 2\bar{N}_d + 1$ , indicates that  $d_{c=2}^*(N_h) \leq \bar{N}_d$ . Therefore,

$$g(N_h) \leq d_{c=2}^*(N_h) \leq \bar{N}_d = d_{s,p}.$$

3) For the case of  $k \geq \bar{N}_d + 2$ , (28) becomes  $d_{c=1}(N_h) = 0$ . Therefore,

$$\begin{aligned} g(N_h) &\leq d_{c=2}^*(N_h) \leq s_2(N_h) \\ &= \min\{N_s, N_s + N_h - N_{ep}\} \\ &\leq 2\bar{N}_d + i - k \leq \bar{N}_d + i - 2 \\ &\leq \bar{N}_d = d_{s,p}. \end{aligned}$$

Based on the above two subcases, i.e., A. 1 and A. 2, one can see that for the case of  $N_s \leq N_{ep}$  the maximum value of  $g(N_h)$  over  $N_h$  is  $g(\hat{N}_h) = g(\bar{N}_h) = d_{s,p}$ . It is worth noting that, although both  $\hat{N}_h$  and  $\bar{N}_h$  can achieve the maximum S.D.o.F., as it can be observed in Section V, for the helper-assisted wiretap channel with the antenna allocation given by  $\hat{N}_h$ , the formulas of the candidate precoding vector pairs are independent of the channel matrices to Bob. Therefore, when the channel estimates are noisy the proposed scheme with  $N_h = \hat{N}_h$  outperforms that scheme with  $N_h = \bar{N}_h$  in terms of the achievable secrecy rate.

#### B. For the case of $N_s > N_{ep}$

It holds that  $\delta = \lfloor \frac{N_{\text{sum}} - |N_s - N_{ep}|}{3} \rfloor + (N_s - N_{ep})$ .

Let  $\hat{N}_d = 2 \lfloor \frac{N_{\text{sum}} - |N_s - N_{ep}|}{3} \rfloor + j + (N_s - N_{ep})$ , and

$$\hat{N}_h = \lfloor \frac{N_{\text{sum}} - |N_s - N_{ep}|}{3} \rfloor, \quad (29)$$

where  $j \triangleq N_{\text{sum}} - 3\hat{N}_d$ . By definition,  $j \in \{0, 1, 2\}$ . Besides, since  $\hat{N}_h < \hat{N}_d$ , it holds that

$$d_{c=1}(\hat{N}_h) = N_s - N_{ep}. \quad (30)$$

##### B. 1 When $\hat{N}_h \geq N_{ep}$

In this subcase, it can be verified that  $N_s \leq \delta$  and  $N_s \leq N_{\text{sum}}$ . Thus, (18) becomes

$$d_{s,p} = N_s. \quad (31)$$

On the other hand, since  $\hat{N}_h \geq N_{ep}$ , it holds that

$$s_2(\hat{N}_h) = N_{ep}. \quad (32)$$

Substituting (30) and (32) into (19) yields  $g(\hat{N}_h) = N_s$ . In addition, by (19) the inequality  $g(N_h) \leq N_s$  always holds true. Therefore, the maximum value of  $g(N_h)$  over  $N_h$  is

$$g(\hat{N}_h) = N_s \stackrel{(a)}{=} d_{s,p},$$

where (a) comes from the equality in (31).

### B. 2 When $\hat{N}_h < N_{ep}$

In this subcase, it can be verified that  $\delta \leq N_s$  and  $\delta \leq N_{\text{sum}}$ . Thus, (18) becomes

$$d_{s,p} = \delta = \hat{N}_h + (N_s - N_{ep}). \quad (33)$$

On the other hand,  $\hat{N}_h < N_{ep}$  combined with (20b), gives

$$d_{c=2}^*(\hat{N}_h) = \hat{N}_h. \quad (34)$$

Substituting (30) and (34) into (19) yields

$$g(\hat{N}_h) = \hat{N}_h + (N_s - N_{ep}) \stackrel{(a)}{=} d_{s,p},$$

where (a) comes from the equality in (33).

In the sequel, we will prove that for any other  $N_h \neq \hat{N}_h$  it holds that  $g(N_h) \leq d_{s,p}$ , thus completing the proof of that the maximum value of  $g(N_h)$  over  $N_h$  is  $g(\hat{N}_h) = d_{s,p}$ .

i) For any  $N_h < \hat{N}_h$ , it holds that  $d_{c=1}(N_h) = N_s - N_{ep}$  and  $d_{c=2}^*(N_h) = N_h < \hat{N}_h$ . Therefore,

$$g(N_h) \leq d_{c=1}(N_h) + d_{c=2}^*(N_h) \leq d_{s,p}. \quad (35)$$

ii) For any  $N_h$  satisfying  $N_h > \hat{N}_h$  and  $N_h \leq N_d$ , it holds that  $d_{c=1}(N_h) = N_s - N_{ep}$ . Based on (20b) it holds that

$$\begin{aligned} d_{c=2}^*(N_h) &\leq \lfloor (N_d - d_{c=1}(N_h))^+ / 2 \rfloor \\ &\leq \lfloor (\hat{N}_h - 1 - d_{c=1}(N_h))^+ / 2 \rfloor \\ &= \hat{N}_h + \lfloor (j - 1) / 2 \rfloor, \end{aligned}$$

which, combined with the fact  $j \leq 2$ , indicates that,  $d_{c=2}^*(N_h) \leq \hat{N}_h$ . Therefore, the inequalities in (35) also hold true.

iii) For any  $N_h$  satisfying  $N_h > \hat{N}_h$  and  $N_h > N_d$ , we will first give a specific value of  $N_h$ , denoted by  $\bar{N}_h$ , which satisfies  $g(\bar{N}_h) \leq d_{s,p}$ . We then prove that for any other  $N_h \neq \bar{N}_h$  it holds that  $g(N_h) \leq g(\bar{N}_h)$ . In this way, we finish the proof that  $g(N_h) \leq d_{s,p}$ .

Note that since  $N_{\text{sum}} = N_h + N_d > 2N_d$ , for the case of  $N_{\text{sum}} \leq 2(N_s - N_{ep})$  it holds that  $N_d < (N_s - N_{ep})$ , which, combined with  $g(N_h) \leq N_d$ , indicates that  $g(N_h) < N_s - N_{ep} < d_{s,p}$ . Therefore, in the following arguments we only need to focus on the case of  $N_{\text{sum}} > 2(N_s - N_{ep})$ .

Let  $\bar{N}_d = \lfloor \frac{N_{\text{sum}} - 2|N_s - N_{ep}|}{3} \rfloor + (N_s - N_{ep})$ , and

$$\bar{N}_h = 2 \lfloor \frac{N_{\text{sum}} - 2|N_s - N_{ep}|}{3} \rfloor + \tau + (N_s - N_{ep}), \quad (36)$$

where  $\tau \triangleq N_{\text{sum}} - 3 \lfloor \frac{N_{\text{sum}} - 2(N_s - N_{ep})}{3} \rfloor - 2(N_s - N_{ep})$ . By definition, it holds that  $\tau \in \{0, 1, 2\}$ .

Substituting (36) into (20a), we arrive at

$$d_{c=1}(\bar{N}_h) = N_s - N_{ep} + \min \left\{ \lfloor \frac{N_{\text{sum}} - 2|N_s - N_{ep}|}{3} \rfloor + \tau, N_{ep} \right\},$$

which, combined with (19), gives

$$g(\bar{N}_h) = \bar{N}_d = \lfloor \frac{N_{\text{sum}} - 2|N_s - N_{ep}|}{3} \rfloor + (N_s - N_{ep}). \quad (37)$$

On comparing (33) and (37), one can see that

$$g(\bar{N}_h) \leq d_{s,p}. \quad (38)$$

On the other hand, for any  $N_h < \bar{N}_h$ , say  $N_h = \bar{N}_h - k$ ,  $k \geq 1$ , it holds that  $N_d = \bar{N}_d + k$ . Thus,  $N_h - N_d = \bar{N}_h - \bar{N}_d - 2k < N_{ep}$ , which together with (20a), indicates that

$$\begin{aligned} d_{c=1}(N_h) &= (N_s - N_{ep}) + \lfloor \frac{N_{\text{sum}} - 2|N_s - N_{ep}|}{3} \rfloor + \tau - 2k \\ &\stackrel{(a)}{=} g(\bar{N}_h) + \tau - 2k, \end{aligned}$$

where (a) is due to (37). In addition, by (20b) we have

$$d_{c=2}^*(N_h) \leq \lfloor (N_d - d_{c=1}(N_h))^+ / 2 \rfloor \leq \lfloor \frac{3k - \tau}{2} \rfloor.$$

Since  $\tau \leq 2$  and  $k \geq 1$ , it holds that  $\tau - 2k + \lfloor \frac{3k - \tau}{2} \rfloor \leq 0$ . Therefore,

$$g(N_h) \leq d_{c=1}(N_h) + d_{c=2}^*(N_h) \leq g(\bar{N}_h). \quad (39)$$

Moreover, for any  $N_h > \bar{N}_h$ , it holds that

$$g(N_h) \leq N_d < \bar{N}_d = g(\bar{N}_h). \quad (40)$$

Combining (39) with (40), one can see that for any other  $N_h \neq \bar{N}_h$  satisfying  $N_h > \hat{N}_h$  and  $N_h > N_d$ , it holds that  $g(N_h) \leq g(\bar{N}_h)$ , which, combined with (38), indicates that  $g(N_h) \leq d_{s,p}$ . This completes the proof.

## APPENDIX C PROOF OF Theorem 1

In the sequel, we will consider three distinct cases.

- 1) For the case of  $N_e^t \geq N_e^r$ , *Eve* cannot see any interference-free subspaces, and so the maximum achievable S.D.o.F. is equal to  $\lim_{P \rightarrow \infty} \frac{R_b}{\log P}$ , whose maximum value over the input covariance matrices is  $\min\{(N_b - N_e^t)^+, N_a\}$ . In that case, there is no need for *Bob* to transmit jamming signals to reduce the interference-free subspace that *Eve* can see, and so we set  $N_b^{t*} = 0$ .
- 2) For the case of  $N_e^t < N_e^r$  and  $N_e^t \geq N_b$  the maximum achievable S.D.o.F. is zero since *Bob* already cannot see any interference-free subspaces. In that case, the achievable S.D.o.F. will be zero even if *Bob* transmits jamming signals, and so we set  $N_b^{t*} = 0$ .
- 3) For the case of  $N_e^t < N_e^r$  and  $N_e^t < N_b$ , no positive S.D.o.F. can be achieved if  $N_b^t \leq N_e^t$ , and thus, in order to maximize the achievable S.D.o.F., *Bob* should choose a value of  $N_b^t$  such that  $N_b^t > N_e^t$ . In that case, and by Proposition 1, one can see that the maximum achievable S.D.o.F. is equal to that of a helper-assisted wiretap channel with number of antennas  $N_s = N_a$ ,  $N_h = N_b^t$ ,  $N_d = N_b^r - N_e^t$ ,  $N_{\text{sum}} = N_b - N_e^t$  and  $N_{ep} = N_e^r - N_e^t$ . Substituting these values into Proposition 2, we arrive at we arrive at the expression of  $N_b^{t*}$ , i.e.,  $\hat{N}_h$ , and also the maximum achievable S.D.o.F., i.e.,  $\min\{\eta, N_b - N_e^t, N_a\}$ .

Concluding the above three cases, one can obtain the expressions of  $d_{s,a}(N_e^t)$  and  $N_b^{t*}$ , as given in (6) and (7), respectively. This completes the proof.

APPENDIX D  
PROOF OF Theorem 2

We should note that for the case of  $N_e \geq N_b$ , the best choice for *Eve* is to allocate  $N_b$  antennas to transmit; for that case no positive S.D.o.F. can be achieved. In what follows, we only need to study the nontrivial case of  $N_e < N_b$ .

From (6), one can see that the achievable S.D.o.F. for the case of  $N_e^r < N_e^t$  is no greater than that of the other case. Therefore, to make sure that the achievable S.D.o.F. is minimized, *Eve* would always choose the value of  $N_e^t$  such that  $N_e^t < N_e^r$ ; for that case

$$d_{s,a}(N_e^t) = \min\{\eta, N_b - N_e^t, N_a\}, \quad (41)$$

with  $\eta \triangleq \lfloor \frac{(N_b - N_e^t - |N_a - N_e^r + N_e^t|)^+}{3} \rfloor + (N_a - N_e^r + N_e^t)^+$ .

Looking into the expression of  $\eta$ , we get two thresholds of  $N_e^t$ , i.e.,  $\frac{N_e - N_a}{2}$  and  $\frac{N_b + N_e - N_a}{3}$ . Since  $N_e < N_b$ , it holds that  $\frac{N_e - N_a}{2} < \frac{N_b + N_e - N_a}{3}$ . In order to simply the expression of  $d_{s,a}(N_e^t)$ , in the following we will consider three distinct cases, which are obtained by those two thresholds.

1) For the case of  $N_e^t \leq \frac{N_e - N_a}{2}$ , it holds that

$$\eta = \lfloor \frac{N_b + N_a - N_e + N_e^t}{3} \rfloor \leq \lfloor \frac{N_b - N_e^t + N_a + N_e}{3} \rfloor \stackrel{(a)}{\leq} N_b - N_e^t,$$

where (a) comes from the fact that

$$N_a + N_e \leq 2(N_e - N_e^t) < 2(N_b - N_e^t).$$

Thus, (41) becomes

$$m_1(N_e^t) = \min\{\lfloor \frac{N_b + N_a - N_e + N_e^t}{3} \rfloor, N_a\}.$$

2) For the case of  $\frac{N_e - N_a}{2} < N_e^t < \frac{N_b + N_e - N_a}{3}$ , it holds that

$$\eta = \lfloor \frac{N_b - N_a + N_e}{3} \rfloor + N_a - N_e + N_e^t.$$

In addition, due to  $N_e^t < \frac{N_b + N_e - N_a}{3}$  it holds that

$$\begin{aligned} 2N_e^t &\leq 2\lfloor \frac{N_b + N_e - N_a}{3} \rfloor \\ \Rightarrow 2N_e^t &< N_b + N_e - N_a - \lfloor \frac{N_b + N_e - N_a}{3} \rfloor \\ \Rightarrow \lfloor \frac{N_b + N_e - N_a}{3} \rfloor + N_a - N_e + N_e^t &< N_b - N_e^t. \end{aligned}$$

Thus, (41) becomes

$$m_2(N_e^t) = \min\{\lfloor \frac{N_b + N_e - N_a}{3} \rfloor + N_a - N_e + N_e^t, N_a\}.$$

3) For the case of  $N_e^t \geq \frac{N_b + N_e - N_a}{3}$ , it holds that

$$\eta = N_a - N_e + 2N_e^t.$$

Besides, it holds that  $N_b - N_e^t \leq N_a - N_e + 2N_e^t$ , which, combined with  $2N_e^t < N_e$ , indicates that  $N_b - N_e^t < N_a$ . Thus, (41) becomes

$$m_3(N_e^t) = N_b - N_e^t.$$

Concluding the above three cases, one can see that

$$d_{s,a}^{\text{wc}} = \min_{0 \leq N_e^t \leq N_e} \min\{m_1(N_e^t), m_2(N_e^t), m_3(N_e^t)\}. \quad (42)$$

In the sequel, we will consider three distinct cases, according to whether  $m_i(N_e^t)$ ,  $i = 1, 2, 3$ , is feasible. For example, for the case of  $N_e < N_a$ ,  $m_1(N_e^t)$  is infeasible, since by definition it ranges  $N_e^t \leq \frac{N_e - N_a}{2} < 0$  which is unavailable.

A. When  $\max\{\frac{N_b - N_a}{2}, N_a\} \leq N_e < N_b$

It holds that  $\frac{N_e - N_a}{2} \geq 0$  and  $\frac{N_b + N_e - N_a}{3} \leq N_e$ , which indicates that both  $m_1(N_e^t)$  and  $m_3(N_e^t)$  are feasible. Moreover,

$$\begin{aligned} \min_{N_e^t \leq \frac{N_e - N_a}{2}} m_1(N_e^t) &= m_1(0) = \min\{\lfloor \frac{N_b + N_a - N_e}{3} \rfloor, N_a\}, \\ \min_{N_e^t \geq \frac{N_b + N_e - N_a}{3}} m_3(N_e^t) &= m_3(N_e) = N_b - N_e. \end{aligned}$$

As to  $m_2(N_e^t)$ , it is feasible only for the case of  $\lfloor \frac{N_e - N_a}{2} \rfloor + 1 < \frac{N_b + N_e - N_a}{3}$ , in which

$$\begin{aligned} \min_{\frac{N_e - N_a}{2} \leq N_e^t \leq \frac{N_b + N_e - N_a}{3}} m_2(N_e^t) &= m_2(\frac{N_e - N_a - \xi}{2} + 1) \\ &= \min\{\lfloor \frac{N_b + N_e - N_a}{3} \rfloor + \frac{N_a - N_e - \xi}{2} + 1, N_a\}. \end{aligned}$$

Here,  $\xi = 1$  if  $N_e - N_a$  is odd and otherwise  $\xi = 0$ .

Since  $N_a \leq N_e < N_b$ , it holds that

$$\lfloor \frac{N_b - N_e + N_a}{3} \rfloor \leq \lfloor \frac{N_b + N_e - N_a}{3} \rfloor - \lfloor \frac{2(N_e - N_a)}{3} \rfloor.$$

In addition, it can be verified that  $\frac{N_e - N_a + \xi}{2} - 1 \leq \lfloor \frac{2(N_e - N_a)}{3} \rfloor$ . Therefore, we have  $m_1(0) \leq m_2(\frac{N_e - N_a - \xi}{2} + 1)$ .

Combining (42) with the above discussions, one can see that for the case of  $\max\{\frac{N_b - N_a}{2}, N_a\} \leq N_e < N_b$ ,

$$\begin{aligned} d_{s,a}^{\text{wc}} &= \min\{m_1(0), m_3(N_e)\} \\ &= \min\{\lfloor \frac{N_b + N_a - N_e}{3} \rfloor, N_b - N_e, N_a\}. \end{aligned}$$

B. When  $\frac{N_b - N_a}{2} \leq N_e < \min\{N_b, N_a\}$

It holds that  $\frac{N_e - N_a}{2} < 0$  and  $\frac{N_b + N_e - N_a}{3} \leq N_e$ , which indicates that  $m_3(N_e^t)$  is feasible and  $m_1(N_e^t)$  is infeasible. Moreover,

$$\min_{N_e^t \geq \frac{N_b + N_e - N_a}{3}} m_3(N_e^t) = m_3(N_e) = N_b - N_e.$$

$m_2(N_e^t)$  is feasible only for the case of  $N_b - N_a + N_e > 0$ , in which case it holds that

$$\begin{aligned} \min_{N_e^t \geq \frac{N_b + N_e - N_a}{3}} m_2(N_e^t) &= m_2(0) \\ &= \min\left\{\left\lfloor \frac{N_b + N_e - N_a}{3} \right\rfloor + N_a - N_e, N_b - N_e\right\}. \end{aligned}$$

Combining (42) with the above discussions, we have the following conclusions:

- 1) For the case of  $\frac{N_b - N_a}{2} \leq N_e < \min\{N_b, N_a\}$  and  $N_b - N_a + N_e > 0$ , it holds that

$$d_{s,a}^{\text{wc}} = \min\left\{\left\lfloor \frac{N_b + N_e - N_a}{3} \right\rfloor + N_a - N_e, N_b - N_e\right\}.$$

- 2) For the case of  $\frac{N_b - N_a}{2} \leq N_e < \min\{N_b, N_a\}$  and  $N_b - N_a + N_e \leq 0$ , it holds that

$$d_{s,a}^{\text{wc}} = N_b - N_e.$$

C. When  $N_e < \min\{\frac{N_b - N_a}{2}, N_b\}$

It holds that  $\frac{N_b + N_e - N_a}{3} > N_e$ , which indicates that  $m_3(N_e^t)$  is infeasible, and  $m_2(N_e^t)$  is feasible.

$m_1(N_e^t)$  is feasible only for the case of  $N_e \geq N_a$ , in which case it holds that

$$\begin{aligned} d_{s,a}^{\text{wc}} &= \min\{m_1(0), m_2(\frac{N_e - N_a - \xi}{2} + 1)\} \\ &\stackrel{(a)}{=} m_1(0) \stackrel{(b)}{=} N_a. \end{aligned}$$

where (a) is due to  $m_1(0) \leq m_2(\frac{N_e - N_a - \xi}{2} + 1)$ . (b) is due to the fact that  $\left\lfloor \frac{N_b + N_a - N_e}{3} \right\rfloor \geq N_a$ , which is due to  $2N_e < N_b - N_a$  and  $N_e \geq N_a$ .

Also, for the case of  $N_e < N_a$ , we have

$$\begin{aligned} d_{s,a}^{\text{wc}} &= m_2(0) \\ &= \min\left\{\left\lfloor \frac{N_b + N_e - N_a}{3} \right\rfloor + N_a - N_e, N_a\right\} \\ &= N_a. \end{aligned}$$

Concluding, for the case of  $N_e < \min\{\frac{N_b - N_a}{2}, N_b\}$ , it holds that  $d_{s,a}^{\text{wc}} = N_a$ . This completes the proof.

## REFERENCES

- [1] J. Li and A. P. Petropulu, "Optimal input covariance for achieving secrecy capacity in Gaussian MIMO wiretap channels," in *Proc. IEEE ICASSP*, Dallas, Texas, USA, Mar. 2010, pp. 3362–3365.
- [2] —, "Explicit solution of worst-case secrecy rate for MISO wiretap channels with spherical uncertainty," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3892–3895, Jul. 2012.
- [3] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-II: the MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [4] S. A. A. Fakoorian and A. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO gaussian wiretap channel," in *Proc. IEEE ISIT*, Cambridge, MA, Jul. 2012, pp. 2321–2325.
- [5] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE VTC'05 Fall*, Texas, USA, 2005, pp. 1906–1910.
- [6] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.
- [7] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.
- [8] H.-T. Chiang and J. S. Lehnert, "Optimal cooperative jamming for security," in *Proc. IEEE MILCOM*, Baltimore, MD, Nov. 2011, pp. 125–130.
- [9] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.
- [10] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
- [11] J. H. Lee and W. Choi, "Multiuser diversity for secrecy communications using opportunistic jammer selection: secure DoF and jammer scaling law," *IEEE Trans. Signal Process.*, vol. 62, no. 4, pp. 828–839, Feb. 2014.
- [12] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
- [13] L. Li, Z. Chen, D. Zhang, and J. Fang, "A full-duplex Bob in the MIMO Gaussian wiretap channel: scheme and performance," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 107–111, Jan. 2016.
- [14] X. Zhou, B. Maham, and A. Hjørungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.
- [15] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. ASILOMAR*, Pacific Grove, CA, Nov. 2011, pp. 265–269.
- [16] A. Garnaev and W. Trappe, "To eavesdrop or jam, that is the question," *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 129, pp. 146–161, Jan. 2014.
- [17] D. Kapetanović, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.
- [18] A. Al-nahari, "Physical layer security using massive multiple-input and multiple-output: passive and active eavesdroppers," *IET Commun.*, vol. 10, no. 1, pp. 50–56, 2016.
- [19] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission in the presence of an active eavesdropper," in *Proc. IEEE ICC*, London, England, Jun. 2015, pp. 1434–1440.
- [20] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "A game theoretic analysis of secret and reliable communication with active and passive adversarial modes," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2155–2163, Mar. 2016.
- [21] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 82–91, Jan. 2013.
- [22] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Basar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," in *Proc. IEEE Military Communications Conference*, Baltimore, USA, Nov. 2011, pp. 119–124.
- [23] M. R. Javan, "Guaranteeing secure communication in OFDM network with an active eavesdropper," in *Proc. IEEE International Symposium on Telecommunications*, Tehran, Iran, Sep. 2014, pp. 868–872.
- [24] A. Sabharwal, P. Schniter, and et. al., "In-band full-duplex wireless: challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.
- [25] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.
- [26] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.
- [27] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, 4th ed. Cambridge University Press, 2006.
- [28] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4971, Aug. 2011.
- [29] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," *EURASIP J. Wireless Commun. and Net.*, vol. 2009, no. 5, pp. 1–13, Mar. 2009.

- [30] L. Li, Z. Chen, J. Fang, and A. P. Petropulu, "Secrecy degrees of freedom of a MIMO Gaussian wiretap channel with a cooperative jammer," in *Proc. IEEE ICASSP*, Shanghai, China, Mar. 2016, pp. 3486–3490.
- [31] L. Li, A. P. Petropulu, Z. Chen, and J. Fang, "Improving wireless physical layer security via exploiting co-channel interference," *to appear in IEEE J. Sel. Topics Signal Process.*
- [32] H. Inaltekin, M. Chiang, H. V. Poor, and S. B. Wicker, "On unbounded path-loss models: Effects of singularity on wireless network performance," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1078–1092, Sep. 2009.
- [33] B. Nosrat-Makouei, J. G. Andrews, and R. W. Heath, "MIMO interference alignment over correlated channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2783–2794, Jun. 2011.